

**What Is Claimed Is:**

- 1        1.        A method to facilitate global timeout in a distributed computing  
2        environment, comprising:
  - 3            receiving an access request from a user at an application in the distributed  
4        computing environment;
  - 5            determining if the distributed computing environment has issued an  
6        authentication to a user device through which the user accesses the application,  
7        wherein the authentication is stored within a time-stamped token on the user-  
8        device, and wherein the authentication has not expired; and  
9            if the authentication has not been received or has expired, redirecting the  
10       access request to a single sign-on server for the distributed computing  
11       environment;
  - 12            otherwise granting access to the application to the user.
- 1        2.        The method of claim 1, wherein the distributed computing  
2        environment includes multiple partner applications distributed across multiple  
3        network servers coupled to a public network.
- 1        3.        The method of claim 2, wherein the public network includes the  
2        Internet.
- 1        4.        The method of claim 2, wherein determining if the distributed  
2        computing environment has issued the authentication to the user involves:

3 receiving an authentication credential from the user;  
4 verifying that the authentication credential is valid; and  
5 providing the time-stamped token to the user-device, wherein the time-  
6 stamped token includes the authentication and a time.

1 5. The method of claim 4, wherein determining if the authentication  
2 has expired involves:

3 recovering the time-stamped token from the user-device;  
4 adding the specified period to the time within the time-stamped token to  
5 produce an expiry time; and  
6 detecting if a current time is later than the expiry time, whereby if the  
7 current time is later than the expiry time, the authentication has expired.

1 6. The method of claim 5, wherein the time within the time-stamped  
2 token is updated to the current time by a partner application when the partner  
3 application is accessed.

1 7. The method of claim 4, wherein the time-stamped token is a  
2 domain cookie, wherein the domain cookie is accessible by multiple network  
3 servers within a domain on the public network.

1 8. The method of claim 4, wherein the time-stamped token is  
2 encrypted to prevent attacks.

1           9.     A computer-readable storage medium storing instructions that  
2     when executed by a computer cause the computer to perform a method to  
3     facilitate global timeout in a distributed computing environment, the method  
4     comprising:

5                 receiving an access request from a user at an application in the distributed  
6     computing environment;

7                 determining if the distributed computing environment has issued an  
8     authentication to a user device through which the user accesses the application,  
9     wherein the authentication is stored within a time-stamped token on the user-  
10    device, and wherein the authentication has not expired; and

11                if the authentication has not been received or has expired, redirecting the  
12    access request to a single sign-on server for the distributed computing  
13    environment;

14                otherwise granting access to the application to the user.

1           10.    The computer-readable storage medium of claim 9, wherein the  
2     distributed computing environment includes multiple partner applications  
3     distributed across multiple network servers coupled to a public network.

1           11.    The computer-readable storage medium of claim 10, wherein the  
2     public network includes the Internet.

1           12. The computer-readable storage medium of claim 10, wherein  
2 determining if the distributed computing environment has issued the  
3 authentication to the user involves:  
4           receiving an authentication credential from the user;  
5           verifying that the authentication credential is valid; and  
6           providing the time-stamped token to the user-device, wherein the time-  
7 stamped token includes the authentication and a time.

1           13. The computer-readable storage medium of claim 12, wherein  
2 determining if the authentication has expired involves:  
3           recovering the time-stamped token from the user-device;  
4           adding the specified period to the time within the time-stamped token to  
5 produce an expiry time; and  
6           detecting if a current time is later than the expiry time, whereby if the  
7 current time is later than the expiry time, the authentication has expired.

1           14. The computer-readable storage medium of claim 13, wherein the  
2 time within the time-stamped token is updated to the current time by a partner  
3 application when the partner application is accessed.

1           15. The computer-readable storage medium of claim 12, wherein the  
2 time-stamped token is a domain cookie, wherein the domain cookie is accessible  
3 by multiple network servers within a domain on the public network.

1           16.    The computer-readable storage medium of claim 12, wherein the  
2    time-stamped token is encrypted to prevent attacks.

1           17.    An apparatus to facilitate global timeout in a distributed computing  
2    environment, comprising:

3                a receiving mechanism that is configured to receive an access request from  
4    a user at an application in the distributed computing environment;  
5                a determining mechanism that is configured to determine if the distributed  
6    computing environment has issued an authentication to a user device through  
7    which the user accesses the application, wherein the authentication is stored  
8    within a time-stamped token on the user-device, and wherein the authentication  
9    has not expired; and

10               a redirecting mechanism that is configured to redirect the access request to  
11    a single sign-on server for the distributed computing environment if the  
12    authentication has not been received or has expired.

1           18.    The apparatus of claim 17, wherein the distributed computing  
2    environment includes multiple partner applications distributed across multiple  
3    network servers coupled to a public network.

1           19.    The apparatus of claim 18, wherein the public network includes the  
2    Internet.

1           20. The apparatus of claim 18, wherein the receiving mechanism is  
2 further configured to receive an authentication credential from the user, the  
3 apparatus further comprising:

4           a verifying mechanism that is configured to verify that the authentication  
5 credential is valid; and

6           a time-stamp mechanism that is configured to provide the time-stamped  
7 token to the user-device, wherein the time-stamped token includes the  
8 authentication and a time.

1           21. The apparatus of claim 20, further comprising:

2           a recovering mechanism that is configured to recover the time-stamped  
3 token from the user-device;

4           an adding mechanism that is configured to produce the specified period to  
5 the time within the time-stamped token to produce an expiry time; and

6           a detecting mechanism that is configured to detect if a current time is later  
7 than the expiry time, whereby if the current time is later than the expiry time, the  
8 authentication has expired.

1           22. The apparatus of claim 21, wherein the time within the time-  
2 stamped token is updated to the current time by a partner application when the  
3 partner application is accessed.

1           23.     The apparatus of claim 20, wherein the time-stamped token is a  
2     domain cookie, wherein the domain cookie is accessible by multiple network  
3     servers within a domain on the public network.

1           24.     The apparatus of claim 20, wherein the time-stamped token is  
2     encrypted to prevent attacks.